IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA,

v.

Criminal No. 1:23cr97 (DJN)

MOHAMMED AZHARUDDIN CHHIPA,
Defendant.

MEMORANDUM OPINION
(Denying Defendant's Motions to Suppress)

This matter comes before the Court on Defendant Mohammed Azharuddin Chhipa's motion to suppress Foreign Intelligence Surveillance Act ("FISA") and FISA Amendment Acts ("FAA" or "Section 702") material and fruits thereof and compel disclosure of all surveillance material (ECF No. 111 ("Motion to Suppress FISA Material" or "FISA Motion")) and Chhipa's related motion to suppress the fruits of undisclosed unlawful searches (ECF No. 155 ("Motion to Suppress Fruits of Unlawful Searches")) (collectively, "Motions"). For the following reasons, the Court hereby DENIES Defendant's Motion to Suppress FISA Material (ECF No. 111) and Motion to Suppress Fruits of Unlawful Searches (ECF No. 155).

I. BACKGROUND

The Government charges Chhipa, a naturalized U.S. citizen living in Fairfax, Virginia before his arrest, in a five-count Indictment with Conspiracy to Provide Material Support to a Foreign Terrorist Organization, in violation of 18 U.S.C. § 2339B (Count One), and Material Support of a Foreign Terrorist Organization in violation of 18 U.S.C. § 2339B (Counts Two through Five). The charges in this case stem from allegations that Chhipa collected and sent money to a woman in Syria to benefit the Islamic State of Iraq and al-Sham (ISIS), a designated

Foreign Terrorist Organization. Specifically, the Indictment alleges that in 2021 and 2022 Chhipa sent a total of $840.00 to Unindicted Co-Conspirator 1 ("UCC-1"), a British-born ISIS member residing in Syria.

The FBI began its investigation into Chhipa in October 2008 after Chhipa, while trying to cross the border into Canada, expressed interest in fighting with his Muslim brothers overseas and sympathy for jihadist viewpoints. [redacted]

In March 2019, the Government re-opened the criminal case against Chhipa after an FBI-Miami agent conducting research on a pro-ISIS Facebook page observed the Carl Johnson account "liking" radical, pro-ISIS content and then, upon viewing the Carl Johnson account, observed publicly-available radical, pro-ISIS posts. Once the FBI-Miami agent realized the connection to the closed Washington Field Office ("WFO") investigation into Chhipa, she sent her research to the WFO, which then submitted an emergency disclosure request to Facebook for information about the Carl Johnson account. The WFO also re-opened the FBI investigation into Chhipa.

Facebook closed the Carl Johnson account in early April 2019, because the account violated Facebook's terms of service. In response, Chhipa created new accounts with different

aliases, which the FBI identified through an online convert employee ("OCE") who had previously connected with the Carl Johnson account. During this time, the Government submitted subpoenas to Facebook for subscriber information and also sought information from other service providers concerning the information that it received from Facebook, including by making requests to email service providers for information about the email addresses associated with the relevant Facebook accounts.

[redacted]

1 [redacted]

2 [redacted]

Chhipa now moves to suppress any and all evidence obtained pursuant to FISA and Section 702, as well as for disclosure of the underlying applications for FISA warrants, Section 702 material and notice of all other surveillance programs used.

II. LEGAL STANDARD

FISA establishes procedures for the Government, acting through the Attorney General, to obtain judicial warrants for electronic surveillance or physical searches in the United States to acquire foreign intelligence information. 50 U.S.C. §§ 18041(a)(1), 1804(a)(6)(B), 1823(a)(6)(B). In certain emergency circumstances, the Government may obtain judicial approval after beginning surveillance or conducting a search. *Id.* §§ 1804(a)(1)–(9), 1805(e)(1), 1824(e)(1). Generally, however, the Government first applies to the FISC for a warrant to conduct a search or surveillance. *Id.* § 1803(a)(1).

The Government's application to conduct electronic surveillance must include, *inter alia*, "a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power," "a statement of the proposed minimization procedures," and "a certification . . . of a high-ranking official." *Id.* § 1804(a). An application to conduct a physical search pursuant to FISA must also contain a certification and a statement of proposed minimization procedures, as well as a statement of the facts and circumstances justifying an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that each "premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from" the target. *Id.* § 1823(a)(l)–(8), (a)(3)(B), (C).

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention and dissemination of non-publicly available information concerning non-consenting U.S. persons that the Government obtained through FISA-authorized electronic surveillance or physical search. FISA requires that the Government "reasonably design[]" such minimization procedures to "minimize the acquisition and retention, and prohibit the dissemination" of information concerning non-consenting U.S. persons "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." *Id.* §§ 1801(h)(1), 1821(4)(A). Both the Fourth Circuit and the Eastern District of Virginia, in addressing minimization, have acknowledged that "courts have construed 'foreign intelligence information' broadly and sensibly [and] allowed the government some latitude in its determination of what is foreign intelligence information," *United States v. Rosen*, 447 F. Supp. 2d 538, 551 (E.D. Va. 2006), as "[i]t is not always immediately clear" whether a particular conversation must be minimized because a "conversation that seems innocuous on one day may later turn out to be of great significance[.]" *United States v. Hammoud*, 381 F.3d 316, 334 (4th Cir. 2004), *vacated on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005). Indeed, Congress drafted FISA with the intent to provide "latitude" to the Government. *Rosen*, 447 F. Supp. 2d at 552 (citing H.R. Rep. No. 95-1283, pt. 1, at 58).

The degree to which the Government must minimize information varies in each investigation. For instance, the Government may engage in less minimization at acquisition when "the investigation is focusing on what is thought to be a widespread conspiracy" and requires more extensive surveillance "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d 717, 741 (FISC Ct. Rev. 2002); *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D.N.Y. 2000) (stating that "more extensive monitoring and greater leeway

in minimization efforts are permitted . . . given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted"). Absent claims that the minimization procedures were disregarded completely, courts inquire whether the Government attempted a good faith effort to minimize. *Rosen*, 447 F. Supp. 2d at 551; *see also Hammoud*, 381 F.3d at 334 ("The minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information."). FISA does not mandate that the Government minimize information that constitutes "evidence of a crime," even if it does not qualify as foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c).

In the requisite certification, a high-ranking executive branch official with national security responsibilities must certify that, *inter alia*, "the information sought [constitutes] foreign intelligence information," "a significant purpose of the surveillance is to obtain foreign intelligence information," and "such information cannot reasonably be obtained by normal investigative techniques." *Id.* § 1804(a)(6). The certifications should be "subjected only to minimal scrutiny by the courts," *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987), and should be afforded a "presumption of validity." *United States v. Hassan*, 742 F.3d 104, 138–39 (4th Cir. 2014). For U.S. persons like Chhipa, the certifications may not be "clearly erroneous." 50 U.S.C. §§ 1805(a)(4), 1824(a)(4); *Badia*, 827 F.2d at 1463.

After the Attorney General has approved an application for electronic surveillance and/or physical search under FISA, the FISC considers it. 50 U.S.C. §§ 1804(a), 1823(a). The FISC may only approve the requested surveillance/search upon a finding that, *inter alia*, there exists:

> probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power, or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power[.]

Id. §§ 1805(a)(l)–(4), 1824(a)(l)–(4). Further, the FISC must also find that the "proposed minimization procedures meet the statutory requirements," the application contains all of the required statements and certifications, and "if the target is a United States person, the certifications are not clearly erroneous." *Id.* If the FISC makes all necessary findings and concludes the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance and/or physical search requested in the application. *Id.* §§ 1805(a), 1824(a).

Once the Government has obtained information from a FISA search or surveillance, it may use this information in a criminal prosecution only if it obtains advance authorization from the Attorney General and provides proper notice to the court and to the "aggrieved person" against whom it seeks to use the information. 50 U.S.C. §§ 1806(b)–(d), 1825(c)–(e). An aggrieved person may, as Chhipa has, move to suppress the use of FISA information on the grounds that the Government unlawfully acquired the information or did not make the surveillance or search in conformity with an order of authorization or approval. *Id.* §§ 1806(e), 1825(f). In addition, a defendant, as Chhipa has here, may file a motion or request under any other statute or rule of the United States to discover or obtain applications, orders or other materials relating to the FISA materials. *Id.* §§ 1806(f), 1825(g).

FISA provides that a motion to suppress or obtain evidence obtained from electronic surveillance or physical search under FISA shall trigger an *in camera, ex parte* review of such material if an appropriate government official files an affidavit that disclosure or an adversary hearing would harm the national security of the United States. 50 U.S.C. §§ 1806(f), 1825(g); *see also* 50 U.S.C. §§ 180l(g), 1821(1) (specifying which government officials may provide such an affidavit). The Government has filed such an affidavit. (ECF No. 124-1 ("Declaration of

Matthew G. Olsen"). Accordingly, the Court "may disclose to [Chhipa]. . . portions of the application, order, or other materials relating to the surveillance [or physical search] only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]." *Id.* §§ 1806(f), 1825(g).

III. ANALYSIS

Defendant expresses frustration that his counsel must draft his Motions "essentially blindfolded," given that neither he nor his counsel have access to the classified surveillance material that the Motions address. (Def. Reply to FISA Mot. at 2.) While the Court acknowledges the challenges facing defense counsel, with FISA, "Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements." *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982). In the context of FISA, "the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization[.]" *Id.* While the relative lack of adversarial briefing differs from the usual context of criminal proceedings, FISA enlists the Court to step into defense counsel's shoes and conduct a fulsome review of the relevant material to ensure compliance with statutory and constitutional constraints. *See United States v. Amawi*, 695 F.3d 457, 471 (6th Cir. 2012) ("Rather than neutrally deciding disputes with an open record based on the adversarial process, [the court] must place [itself] in the shoes of defense counsel, the very ones that cannot see the classified record, and act with a view to their interests.")

In accordance with this mandate, the Court has conducted a careful review of the FISA material at issue to assess whether any of the Government's evidence must be suppressed or

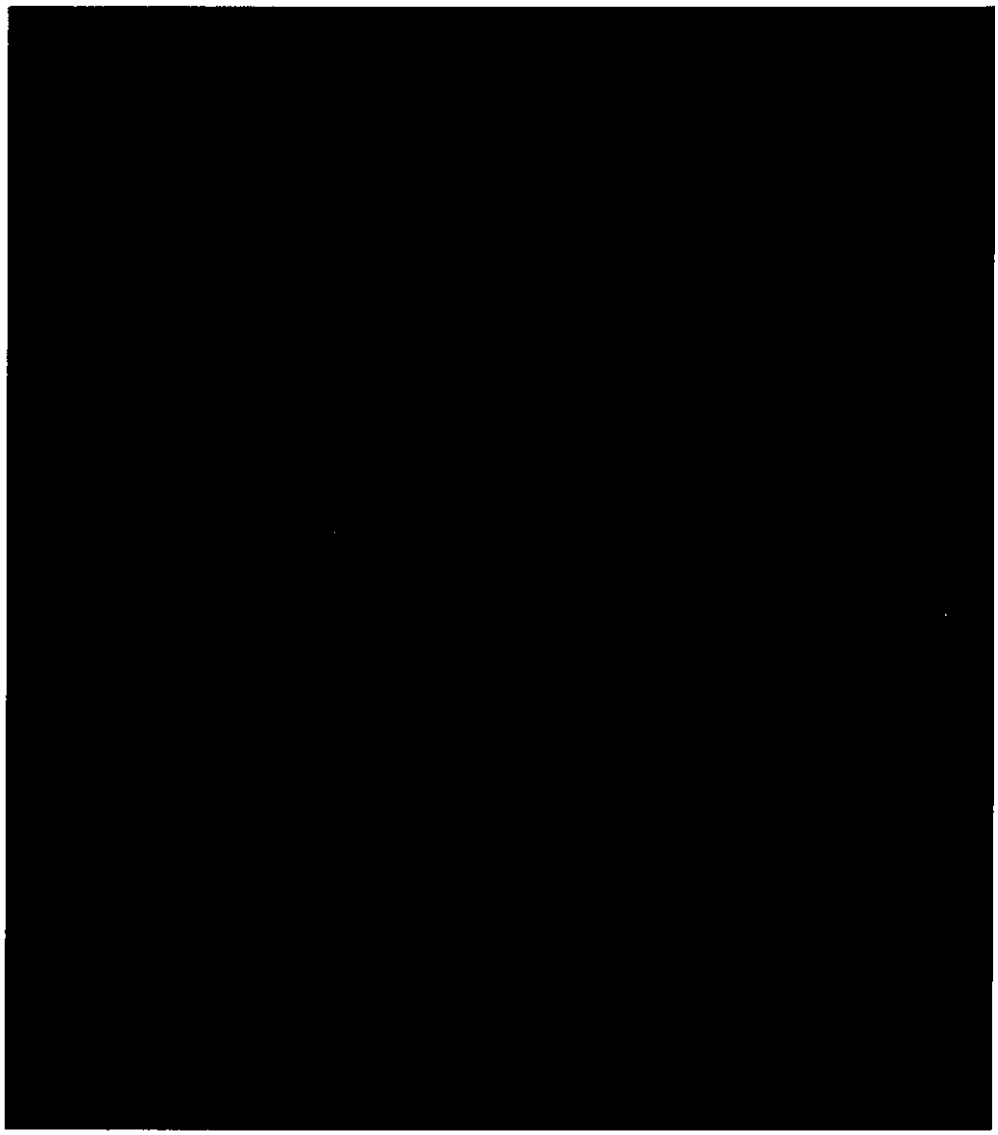
disclosed. The Court summarizes the findings of that review, first addressing the adequacy of the FISA applications, including the establishment of probable cause, provision of the appropriate certifications and adherence to minimization procedures. Then, the Court assesses each of Chhipa's suppression arguments in turn, rejecting each of them in light of the Court's review of the FISA material and the relevant case law and statutory provisions. Finally, the Court addresses Chhipa's requests for disclosure of the FISA material. Upon thorough review of the relevant FISA material and consideration of Defendant's concerns, the Court concludes that the Government lawfully conducted the electronic surveillance and physical search at issue with the appropriate authorizations and that the circumstances neither warrant suppression nor permit disclosure of FISA material to Chhipa.

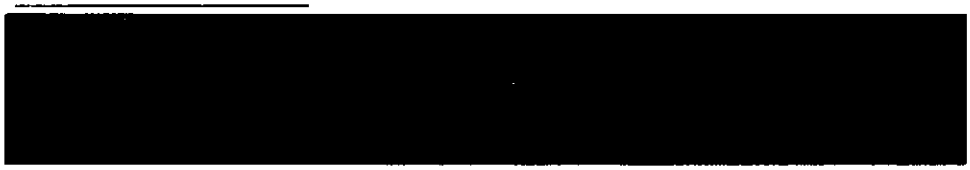
A. Adequacy of the FISA Applications

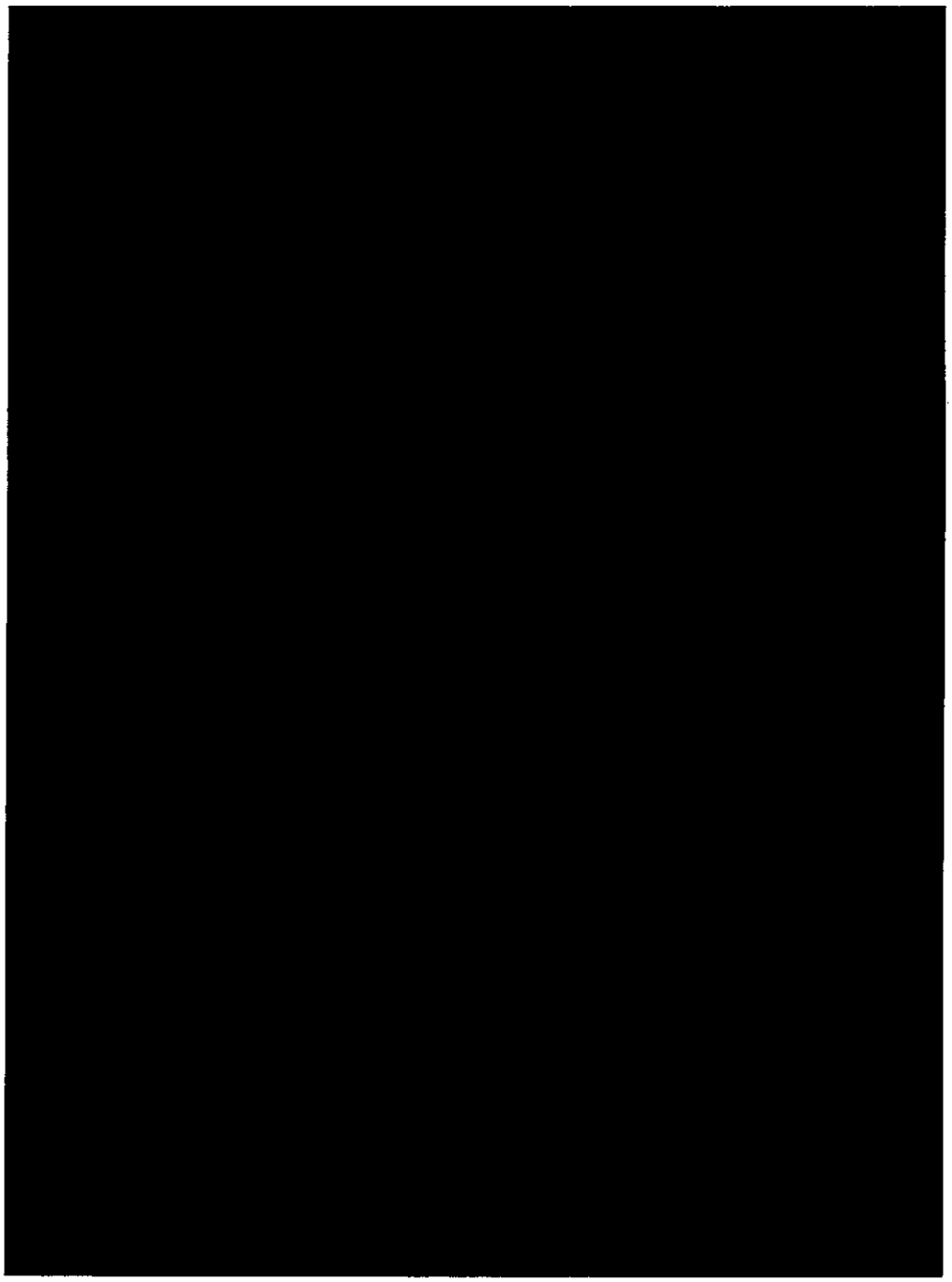
1. Probable Cause

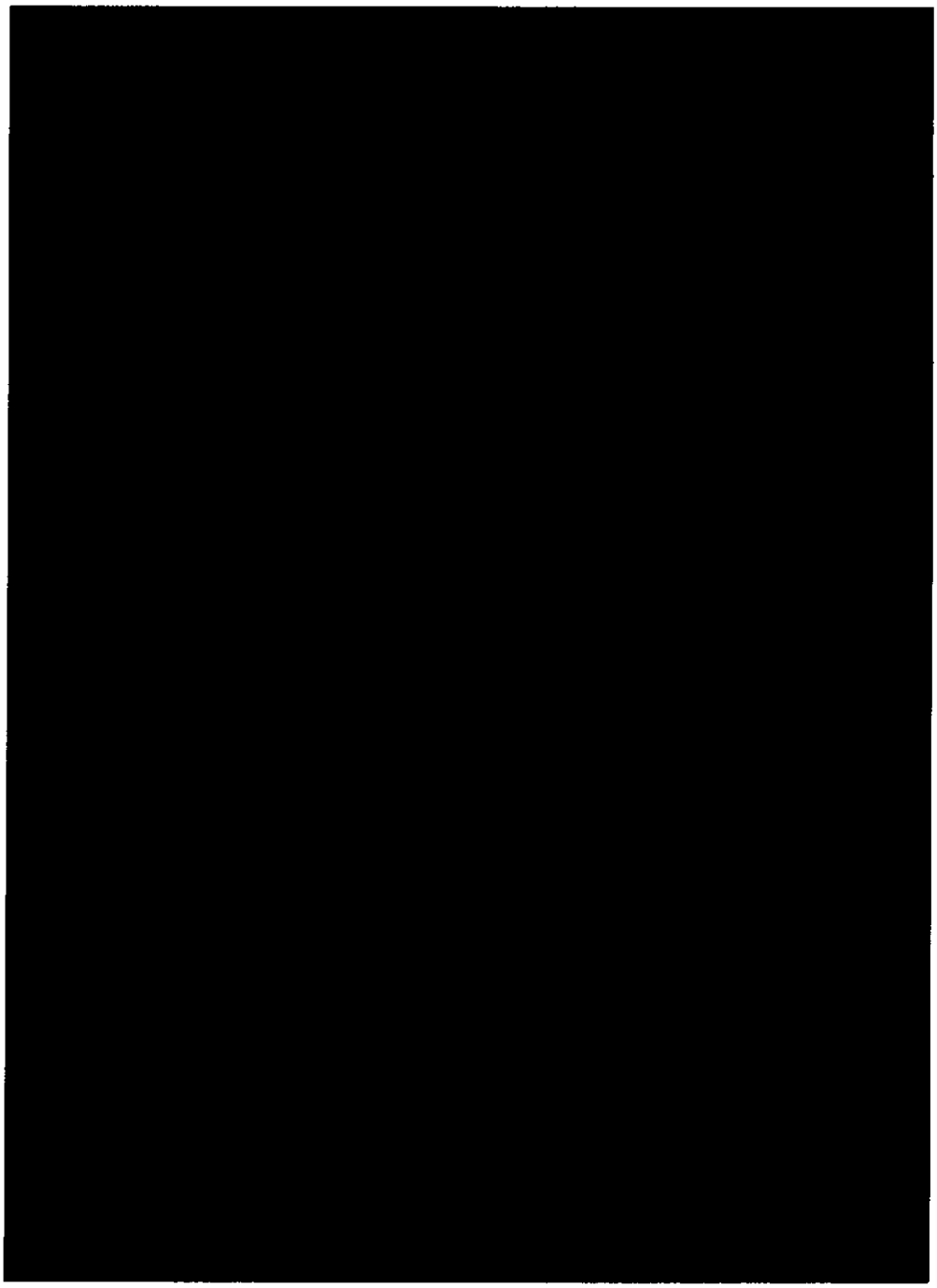
In evaluating the legality of the FISA collection, the Court reviews the FISC's probable cause determination *de novo*. *See Hassan*, 742 F.3d at 138–39 (noting that the district court correctly reviewed the FISA materials "de novo with no deference accorded to" the FISC's probable cause determinations). Upon such review, the Court determines that the FISA applications filed in the dockets at issue demonstrate probable cause to believe that:

[redacted]









[redacted]

2. Minimization

The Court must also assess whether the Government followed the appropriate minimization procedures regarding the acquisition, retention and dissemination of information about Chhipa as a U.S. person. 50 U.S.C. § 1805(a)(3). The Attorney General has adopted Standard Minimization Procedures (SMPs) and incorporated them by reference into every FISA application, including those at issue here. [redacted]

[redacted]

Here, the record indicates that the Government lawfully conducted the FISA collections under the applicable minimization standards. Each FISA application and FISC order reflected that the relevant surveillance and searches were subject to the SMPs.[14] Furthermore, the Government credibly asserts that it then acquired, retained and disseminated the information pursuant to the SMPs and exercised reasonable judgment in determining whether FISA-acquired information should have been minimized. [redacted] (Gov. Opp. to FISA Mot., Exh. 3).) The FBI only conducted surveillances and searches after verifying the existence of an emergency authorization or FISC order covering the relevant facilities, places, premises or property and the relevant timeframe. (*Id.* ¶ 11; SMPs §§ II.A.1, II.B.2 (setting forth the SMPs for acquisition of electronic surveillance and physical searches).) Further, only FBI personnel with authorized access and a need to know reviewed the collected material concerning non-consenting U.S. persons and they did so only as necessary to determine whether such information met the relevant standard described above. [redacted] ¶¶ 14–16.)

Before the Government uploaded any FISA information into general, FBI-wide databases or systems or disseminated it outside of the FBI, the FBI struck or substituted a characterization for any information concerning any U.S. person unless such information met the relevant standard. (*Id.* ¶ 18.) Collectively, this process allowed the Government to subject collected information to two levels of scrutiny before disseminating it. Based on the Government's credible account of its investigation, the Court concludes that the Government lawfully

[redacted]

conducted the FISA collection under the relevant minimization procedures approved by the FISC and applicable to the FISA collection.

3. Certification

Upon review of the applications, the Court finds that the Government properly submitted all required certifications. Each of the FISA applications was supported by a certification signed by a duly authorized, high-ranking official of the U.S. Government. Furthermore, each certification complied with FISA's requirements that the certifying official indicate that the information sought constituted foreign intelligence information, obtaining foreign intelligence information constituted a significant purpose of the surveillance or search, and the information sought could not have reasonably been obtained by normal investigative techniques. *See* 50 U.S.C. §§ 1804(a)(6)(A)–(C), 1823(a)(6)(A)–(C). There exists no reason to think that the certifications were clearly erroneous. To the contrary, the certifications and declarations contained sufficient information and detail to support their claims.

[redacted]

[redacted]

[redacted]

B. Chhipa's Legal Arguments

In his Motions, Chhipa raises concerns that the FISA applications may have: (1) failed to establish probable cause, (2) relied on raw intelligence, (3) relied on illegitimate and/or illegal sources of information, (4) relied on First Amendment protected activity, (5) contained intentional or reckless falsehoods or omissions, (6) omitted the required certifications, and (7) failed to contain or implement the requisite minimization procedures. The Court considered the substance of his first, sixth, and seventh concerns in Section III.A and found that the

[redacted]

Government established probable cause, provided the required certifications and adhered to appropriate minimization procedures. Accordingly, the FISA material ought not be suppressed on those grounds. Regarding certification, however, Chhipa brings an additional challenge to the constitutionality of the significant purpose standard, which the Court address below. Additionally, in this section, the Court will consider Chhipa's claims that the Court ought to suppress the FISA material, because the applications relied on raw intelligence, illegitimate and/or illegal sources of information, intentional or reckless falsehoods or omissions, and First Amendment-protected activities.

1. Raw Intelligence

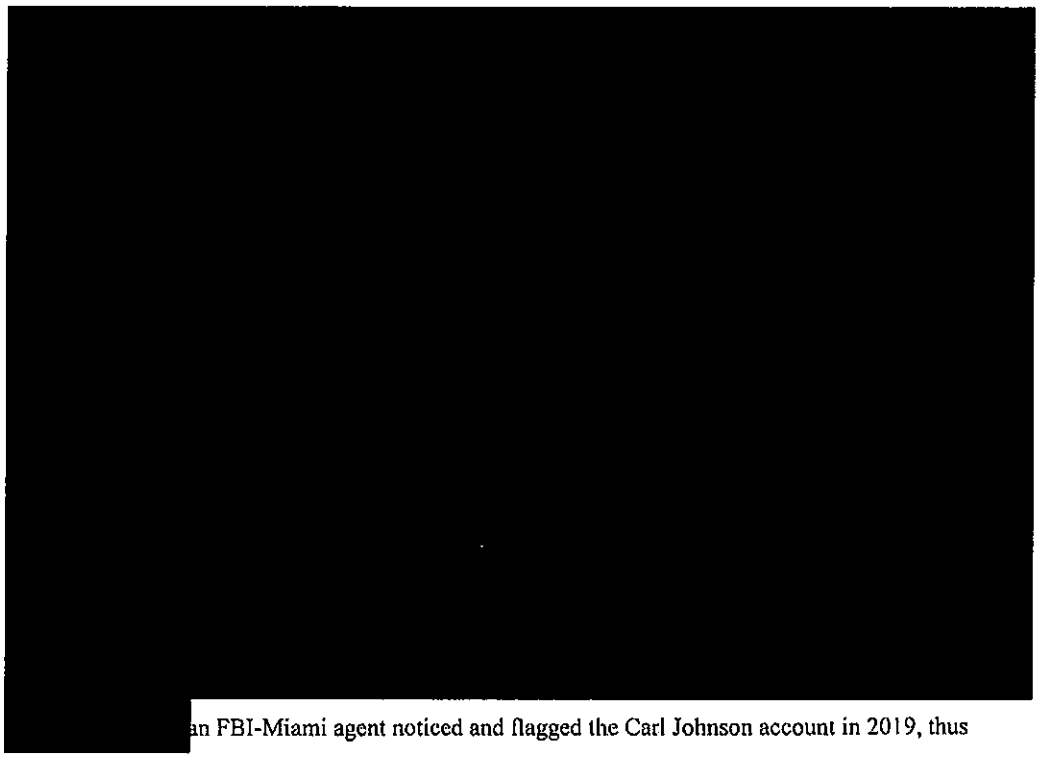
Chhipa raises concerns that the FISA applications at issue contain "raw intelligence" and/or information from foreign intelligence and thus rely on information from unreliable sources lacking independent corroboration. Upon review of the FISA applications at issue, the Court finds such concerns unwarranted. As an initial matter, there exists no "*per se* rule that information contained in an intelligence report is inherently unreliable." *Barhoumi v. Obama*, 609 F.3d 416, 429 (D.C. Cir. 2010). Rather, such information need only "be presented in a form, or with sufficient additional information, that permits . . . [the] court to assess its reliability." *Id.*

[redacted] The relevant FISA applications provided more than sufficient information to corroborate any information that might be considered mere "raw intelligence," and the Government provided sufficient information from reliable sources to establish probable cause in the relevant applications.

2. Illegitimate and/or Illegal Sources of Information

Defendant also argues that virtually all evidence in this case has been tainted by undisclosed, unlawful searches. Specifically, Chhipa claims that the Government engaged in years of searches under Section 702, the Terrorist Surveillance Program ("TSP"), Executive Order 12333 and other means, including warrantless wiretapping, that it has not disclosed to Defendant. To support such arguments, he points to the Government's awareness of the Carl Johnson Facebook account and its ability to connect this account to Chhipa in 2019. Chhipa claims that the account came to the Government's attention in 2019 as a result of unlawful searches, and that the Government only succeeded in linking Chhipa to the account because of such searches. Chhipa argues that the Court must therefore suppress all evidence that the prosecution derived from the Carl Johnson account, including information from the Facebook accounts that the Government only identified through their connection to the Carl Johnson account. Chhipa also asks the Court to compel the Government to disclose the sources of the information contained in the search warrants and FISA warrants.

The Fourth Amendment requires the Court to determine whether the Government acquired the evidence that it intends to introduce at trial as "an indirect result" of an unlawful search and, if so, whether the acquisition of the evidence was nevertheless "so attenuated as to dissipate the taint." *Murray v. United States*, 487 U.S. 533, 536–37 (1988) (citation omitted). Courts must inquire whether the "illegal search" constituted a "but for" cause of the discovery of the challenged evidence, and may conclude that it did not because law enforcement independently discovered that evidence through a source that did not depend on the illegal search or because law enforcement eventually would have discovered it even without the unconstitutional search. *Id.* at 537–39.



an FBI-Miami agent noticed and flagged the Carl Johnson account in 2019, thus forming an independent source for the discovery of the account. The Government has provided FBI records indicating that FBI-Miami agent Janet Waldron began an investigation aimed at reviewing activity related to the Facebook community page "Abu Najm bin al-Iskandar." (ECF No. 168-2 at 4.) While reviewing this community page, Waldron saw the Carl Johnson account expressing support for numerous, alarming Abu Najm bin al-Iskandar posts and, upon reviewing the account, saw that the Carl Johnson account had posted material supportive of ISIS and radical Islam. (*Id.*) Her investigation provides an independent source for the Carl Johnson account to have come to the Government's attention, separate from any surveillance that might have occurred before Waldron's investigation.

The Government also linked the Carl Johnson account to Chhipa independently of any surveillance preceding the Waldron investigation. After Waldron raised concerns about the Carl Johnson account, the FBI requested information about the account from Facebook and received IP address information for the account. (ECF No. 114-4.) The FBI then obtained a subpoena, which allowed it to trace the IP address to Chhipa's home address — the same address that he had provided to U.S. Customs and Border Patrol in 2008. The Government also linked Chhipa to the Carl Johnson account through a Facebook message that he sent saying that his name was Azhar (the first half of Chhipa's middle name) and that he lived in Virginia. [redacted] This explanation is not as flimsy as defense counsel suggests, especially given that the Government possessed lawfully obtained information indicating that Chhipa went by Azhar.[19]

The Government thus would have inevitably been able to link the Carl Johnson account to Chhipa — and, in fact, did so — independent of any [redacted] and search or any other alleged undisclosed surveillance in the intervening decade. Accordingly, even assuming that the Government conducted [redacted] unlawfully or engaged in some other unlawful surveillance of Chhipa or the Carl Johnson account, suppression would not be appropriate in this circumstance. *See Murray*, 487 U.S. at 537 ("When the challenged evidence has an independent source, exclusion of such evidence would put the police in a worse position than they would have been in absent any error or violation.").

[redacted]

As discussed at greater length in Sections I and III.A, the Government established probable cause in its FISC applications and developed its investigation through lawful and disclosed sources. [redacted] Rather, upon review of the FISA material at issue, the Court concludes that the Government developed its investigation and established probable cause through lawful means.

3. First Amendment-Protected Activities

Chhipa raises concerns that the FISA applications at issue relied on First Amendment-protected activity to establish probable cause. (FISA Mot. at 15.) Indeed, no U.S. person may be considered a foreign power or agent of a foreign power based solely on First Amendment-protected activities. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). The FISC may consider First Amendment-protected activities, however, if other activity indicates that a target constitutes an agent of a foreign power. *Rosen*, 447 F. Supp. 2d at 548–49; *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999). Here, the FISA applications at issue establish probable cause through information that does not implicate Chhipa's First Amendment rights, [redacted] To the extent that the applications cite any First Amendment-protected activities, [redacted] thus, do not run afoul of the First Amendment.

4. Intentional or Reckless Falsehoods or Omissions

Chhipa claims that the FISA applications contain intentional or reckless falsehoods or omissions and, correspondingly, seeks a *Franks* hearing, disclosure of the FISA materials and suppression of the FISA information. (FISA Mot. at 16–20.) The Court's review, however, reveals no material false statements or omissions regarding the FISA information that would warrant a hearing or any of the other remedies that Chhipa seeks.

To obtain a *Franks* hearing, a defendant generally must "make 'a substantial preliminary showing that a false statement knowingly or intentionally, or with reckless disregard for the truth, was included' in the application and that the allegedly false statement was 'necessary' to the FISA Judge's approval of the application." *United States v. Duggan*, 743 F.2d 59, 77 & n.6 (2d Cir. 1984) (quoting *Franks*, 438 U.S. at 155–56). Here, Chhipa makes no such showing. He makes a passing reference to an FBI document that references certain facilities —one phone number and two email addresses (ECF No. 114-1 at 9–10) — that he believes the Government could not have been lawfully aware of at the time that they were included in the FBI's records. (FISA Mot. at 20.) But the Government's records provide credible accounts of lawful sources for their knowledge of such facilities.[20, 21] Nor can Chhipa's citations to general violations in

[redacted] the Government knew about the email address (azharc37@gmail.com) that constituted the subject of the March

other FISA cases enable him to meet his burden; as this Court has observed, a summary of generalized errors is no more probative of an error in any one case "than a general study of errors committed over a period of years in baseball would be probative of whether errors occurred in a specific game." *Rosen*, 447 F. Supp. 2d at 552.

Chhipa expresses frustration that he must make such a showing to obtain a *Franks* hearing, given that he does not have access to the FISA material. Recognizing the significant challenges facing defendants who try to make a *Franks* showing, courts review the relevant material in their stead. *See, e.g.*, *Daoud*, 755 F.3d at 483–84 ("[T]he judge makes the additional determination, based on full access to all classified materials and the defense's proffer of its version of events, of whether it's possible to determine the validity of the *Franks* challenge without disclosure of any of the classified materials to the defense."); *United States v. Aziz*, 228 F. Supp. 3d 363, 370 (M.D. Pa. 2017) ("In essence, the court's independent review may supplant that of defense counsel."). As discussed at greater length in Section III.C, this *ex parte*, *in camera* review — not disclosure or an adversarial hearing — provides the appropriate protection for Defendant's rights. Here, based on a careful review of the FISA material, the Court finds no intentional or reckless falsehoods or omissions that would warrant a *Franks* hearing.

5. Significant Purpose Standard

As discussed in Section III.A, the Government made the appropriate certifications and, moreover, the representations in their certifications, including that the collection of foreign intelligence information constituted a significant purpose of the FISA surveillance, easily

20, 2019 grand jury subpoena issued to Google. (ECF No. 114-3.) In his Motion to Suppress FISA Material, Chhipa pointed to the email address in this grand jury subpoena as an unaccounted-for piece of knowledge indicating that the Government had used Section 702 or other unlawful and/or undisclosed means to source information about Chhipa. (FISA Mot. at 51.)

withstand the "minimal scrutiny" to which the Court ought to subject them. *Badia*, 827 F.2d at 1463. In a footnote, however, Chhipa raises an additional challenge to the constitutionality of the significant purpose standard, arguing that it violates the Fourth Amendment. Specifically, he challenges FISA's requirement that the high-ranking government official certify that "a significant purpose of the surveillance is to obtain foreign intelligence information." *Id.* § 1804(a)(6). As Chhipa acknowledges, apart from a vacated decision out of the District of Oregon, every court to have considered the significant purpose test has found it constitutional. *See, e.g.*, *United States v. Abu-Jihaad*, 630 F.3d 102, 128 (2d Cir. 2010) ("FISA's 'significant purpose' requirement . . . is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering . . . . The fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion."); *United States v. Duka*, 671 F.3d 329, 343 (3d Cir. 2011) (finding FISA's "significant purpose" standard constitutional); *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005) (same); *In re Sealed Case*, 310 F.3d at 746 (same); *but see Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007) (finding FISA's "significant purpose" standard unconstitutional), *vacated by Mayfield v. United States*, 599 F.3d 964, 973 (9th Cir. 2010) (finding that the plaintiff lacked standing). This Court agrees with these consistent determinations of the FISA standards' constitutionality in light of the Government's legitimate and special needs for intelligence information.

6. Lapses in Authorization

Chhipa also raises concerns about possible periods of time during which surveillance continued after a FISA order had expired. [redacted]

[redacted] Thus, the Court finds such concerns unwarranted.

7. Section 702 Collection

Defendant further objects to what he calls the Government's "obvious" use of Section 702 and impermissible "backdoor" queries on Chhipa's communications in violation of his Fourth Amendment rights. (FISA Mot. 25–70.) Chhipa asks the Court to suppress any information obtained or derived from this collection under the guise of Section 702. Because the Government does not seek to use Section 702 information in its prosecution, Chhipa lacks standing to bring such a challenge.

Section 702 authorizes the targeting of non-U.S. persons who the Government reasonably believes are outside the United States to acquire foreign intelligence information, but such surveillance may not intentionally target a U.S. person. 50 U.S.C. § 1881a(b)(2). The Government must provide notice that it intends to use or disclose Section 702 information if the Government (1) "intends to enter into evidence or otherwise use or disclose" (2) "against an aggrieved person" (3) in a "trial, hearing or other proceeding in or before any court, department officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) "electronic surveillance of that aggrieved person." 50 U.S.C. §§ 1806(f), 1881e(a). An "aggrieved person" consists of either the target of an electronic surveillance or one whose communications or activities were subject to electronic surveillance. *Id.* §§ 1801(k), 1881e(a). An individual may move to suppress evidence only if he is an aggrieved person in relation to the surveillance or search from which the Government obtained the evidence. *Id.* § 1806(e).

Here, the Government does not seek to use or disclose at trial any Section 702 information. [redacted]

Chhipa's claim stems from a mistaken belief about how the FBI learned of certain facilities; the Court addressed the evidence about which Chhipa expresses skepticism in Sections III.B.2 and III.B.4. The Government provided credible accounts of how it obtained information about Chhipa absent any use of "backdoor quer[ies]," (FISA Mot. at 53), or other methods that Chhipa believes to be unlawful. While the Court appreciates that Chhipa does not have full access to the record and thus understandably startles at shadows that he believes provide

[redacted]

evidence of the Government's unlawful conduct, the Court's *ex parte*, *in camera* review of the classified material at issue does not identify any basis for such fears.

Lastly, the Court finds no issues with the notice that the Government provided. Because Chhipa does not qualify as an aggrieved person under 702, the Government had no reason to provide notice of its FISA use under Section 702. Rather, the Government complied with its notice obligations when it gave notice of its intent to use information obtained or derived from electronic surveillance and physical search conducted pursuant to 50 U.S.C. §§ 1801–12 and 1821–29. (ECF No. 50.)

C. Disclosure

Throughout his Motions, Chhipa argues that he ought to receive the FISA materials under review, so that he may provide input on the legality of the surveillance and searches. But the Court may only disclose the FISA material when "such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). Here, after conducting its *in camera*, *ex parte* review of the materials, the Court has been able to determine the legality of the surveillance or search without defense counsel's assistance and, therefore, does not find disclosure of the material warranted. *See Hassan*, 742 F.3d at 138 ("[W]here the documents submitted by the government [are] sufficient to determine the legality of the surveillance, the FISA materials should not be disclosed.") (quotations omitted). Disclosure constitutes an extraordinary remedy that the circumstances here do not warrant. *See Rosen*, 447 F. Supp. 2d at 546 (recognizing that the "exceptional nature of disclosure of FISA material is especially appropriate in light of the possibility that such disclosure might compromise the ability of the United States to gather foreign intelligence information effectively"). Indeed, as Defendant acknowledges, (FISA Mot. at 72), only one court has ever ordered disclosure of FISA

applications, orders or related material, and the Court of Appeals subsequently overturned that decision. *Daoud*, 755 F.3d 479. Here, the Court finds none of the complicating factors such as "indications of possible misrepresentations of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards" that might suggest an extraordinary case requiring a disclosure or hearing. *Belfield*, 692 F.2d at 147.

Nor do the Federal Rules of Criminal Procedure compel additional notice or disclosure. Congress "intentionally replaced [Rules 12 and 16] with FISA's disclosure framework" and rendered Rule 16 and other existing laws inapplicable to discovery in the FISA context. *United States v. Aziz*, 228 F. Supp. 3d 363, 370 (M.D. Pa. 2017). "Rules 12 and 16 do not, and cannot, supersede FISA's statutory prohibition on disclosure." *Id.* at 370. Even assuming *arguendo* that 18 U.S.C. § 3504 applies to FISA surveillance, *see United States v. Russell*, 2024 WL 4519248 at *3–4 (D. Md. Oct. 17, 2024) (discussing uncertainty in that regard), Chhipa's claims for additional notice and discovery under that provision prove similarly unavailing, as he has not established the requisite "colorable basis" that the Government aggrieved him with unlawful surveillance. *United States v. Apple*, 915 F.3d 899, 905 (4th Cir. 1990); *see United States v. Muhtorov*, 20 F.4th 558, 631 (10th Cir. 2021) (finding a defendant's general, unsupported allegations of unlawful acts were insufficient to trigger the Government's obligation to confirm or deny the use of surveillance techniques under 18 U.S.C. § 3504).

This Court also rejects Chhipa's claims that the adversarial system requires disclosure of FISA materials and that *ex parte* review transgresses such a system. As the Fourth Circuit has previously opined, "Congress did not run afoul of the Constitution when it reasoned that the additional benefit of an unconditional adversarial process was outweighed by the Nation's

interest in protecting itself from foreign threats." *United States v. Dhirane*, 896 F.3d 295, 301 (4th Cir. 2018); *see also United States v. Falvey*, 540 F. Supp. 1306, 1315–16 (E.D.N.Y. 1982) (rejecting constitutional challenges and noting that a "massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera, ex parte* basis); *Daoud*, 755 F.3d 479 (detailing, and deeming appropriate, the federal judiciary's long-standing use of non-adversarial and non-public proceedings in a range of contexts).

Finally, the Court rejects any claim that due process mandates disclosure or additional notice beyond what the Government has provided. As previously discussed, FISA protects a defendant's rights, not through traditional notice or disclosure methods, but through the "in-depth oversight of FISA surveillance by all three branches of government." *Belfield*, 692 F.3d at 148. The resulting multi-branch supervision serves to safeguard defendants' constitutional rights. Indeed, courts have consistently agreed that FISA's *in camera, ex parte* review does not violate the Due Process Clause of the Fifth Amendment, nor does due process require that Chhipa have access to the FISA materials. *See, e.g., United States v. Nicholson*, 955 F. Supp. 588, 592 (E.D. Va. 1997) (finding, based on "the unanimous holdings of prior case law . . . that FISA does not violate the Fifth or Sixth Amendments by authorizing *ex parte* in camera review"). In accordance with FISA's mandate, the Court has carefully reviewed the FISA material and found it lawful. Accordingly, due process does not require disclosure and FISA does not permit it.

Without disclosure, there exists no need for the Court to conduct an evidentiary hearing. As discussed at greater length in Section III.B, Defendant has not made the requisite showing that would entitle him to a *Franks* hearing. Moreover, "[g]iven that disclosure is not necessary

in this case, no purpose would be served by an evidentiary hearing." *Belfield*, 692 F.2d at 147; *see also id.* ("Disclosure and an adversary hearing are the exception, occurring *only* when necessary.") (emphasis in original). Neither the Court nor the Government could disclose more to defense counsel than they already have, and an evidentiary hearing would leave Defendant merely "punching at shadows." *Id.*

* * * *

For the reasons stated above, the Court DENIES Defendant's Motion to Suppress FISA Material (ECF No. 111) and Motion to Suppress Fruits of Unlawful Searches (ECF No. 155). The Court ORDERS that this Memorandum Opinion, the classified versions of the Government's oppositions to Defendants' Motions, and the accompanying classified exhibits shall not be disclosed to the defense and shall be sealed and preserved in the Court's records.

The Court will issue an unclassified Order with its ruling on Defendant's Motions. The Court will provide this Memorandum Opinion explaining the reasoning for its decision to the relevant Classified Information Security Officer (CISO). The Court ORDERS the CISO to deliver the Memorandum Opinion to the Government. The Court ORDERS that, upon receiving the Memorandum Opinion, the Government shall provide a copy to the relevant agencies, which shall review the Memorandum Opinion for classified information. The Court further ORDERS that, no later than November 16, 2024, the Government shall provide Defendant's counsel with a version redacted only as necessary to allow for its review by cleared defense counsel and provide the Court with a separate, declassified version suitable for public release.

It is so ORDERED.

/s/
David J. Novak
United States District Judge

Alexandria, Virginia
Date: November 6, 2024